

The Systematic Normal Form of Lattices

Lior Eldar*

Peter W. Shor†

April 27, 2016

Abstract

We introduce a new canonical form of lattices called the *systematic normal form* (SNF). We show that for every lattice there is an efficiently computable “nearby” SNF lattice, such that for any lattice one can solve lattice problems on its “nearby” SNF lattice, and translate the solutions back efficiently to the original lattice. The SNF provides direct connections between arbitrary lattices, and various lattice related problems like the Shortest-Integer-Solution, Approximate Greatest Common Divisor. As our main application of SNF we derive a new set of worst-to-average case lattice reductions that deviate significantly from the template of Ajtai [2] and improve upon previous reductions in terms of simplicity.

1 Introduction

1.1 The Systematic Normal Form : a “smoothed analysis” of lattices

We introduce a certain canonical form of lattices called the systematic normal form (or SNF for short). An SNF matrix is a matrix of this form:

$$B = \begin{bmatrix} N & b_2 & b_3 & \dots & b_n \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix} \quad (1)$$

where all unspecified entries are 0, and N is a prime number. The SNF form allows for a “smoothed analysis” of lattices in the following sense: Given a matrix B in Hermite normal form (HNF) one can efficiently generate a matrix B_{SNF} in systematic normal form such that any solution of a problem of interest on B_{SNF} can be translated easily to a solution for the original problem on B , albeit with a slight degradation in accuracy. Furthermore, B_{SNF} is in a specialized canonical form with several important properties which are used in the reduction. Hence, the reduction maps each lattice to a “nearby” lattice with the “right” properties.

The defining property of SNF, is that it maps the quotient structure \mathbb{Z}^n/L as a quotient of infinite groups, to a quotient of finite groups \mathbb{F}_N^n/L_N , where $L_N = L \cap \mathbb{F}_N^n$ and $N = \det(B)$. In addition, the very sparse structure of SNF allows for several other important properties among which we name:

*Center for Theoretical physics, MIT

†Department of Mathematics and Center for Theoretical physics, MIT

1. The dual to L_N in \mathbb{F}_N^n , denoted by $(NL^*)_N$ also has a very structured matrix.

$$B = \begin{bmatrix} 1 & & & & \\ -b_2 & 1 & & & \\ -b_3 & & 1 & & \\ \vdots & & & \ddots & \\ -b_n & & & & 1 \end{bmatrix} \quad (2)$$

The duality between these two matrix forms has intriguing connections to well-known problems in cryptography: On one hand, the primal SNF form is shown here to be synonymous with the problem finding short-integer-solutions SIS (see Definition 14, and connection in Proposition 7), whereas solving the closest vector problem on the dual lattice is very similar to the problem of approximate common divisor problem ([18]).

2. It is straightforward to sample uniformly from both L_N and $(NL^*)_N$: to sample uniformly from L_N one samples $n - 1$ coordinates x_n, \dots, x_2 uniformly at random from \mathbb{F}_N , and then sets x_1 as $x_1 = \sum_{i=2}^n b_i x_i \pmod{N}$. For the dual lattice: one samples a uniformly at random from \mathbb{F}_N , and then sets the dual vector as $(a, -b_2 \cdot a \pmod{N}, \dots, -b_n \cdot a \pmod{N})$.
3. For every $x \in \mathcal{P}(L)$, i.e. the basic parallelepiped of L , there exists a unique element in $(NL^*)_N$ that corresponds to x . Furthermore, this element can be computed efficiently from x . This is shown in Claim 1.
4. The SNF form can be naturally associated with a rank-1 instance of SIS modulo a prime number field: Given a vector $g \in \mathbb{F}_N^m$ we define:

$$L(g)_1^\perp := \{h \in \mathbb{F}_N^{m+1}, \langle (1, g), h \rangle = 0 \in \mathbb{F}_N\},$$

One can then show that any SNF matrix B has $L(B) = L(g)_1^\perp$ where g is the vector of non-trivial entries in B , i.e. b_2, \dots, b_n . This is the subject of Proposition 7.

The formal connection between a given lattice basis B and its nearby SNF matrix is given in Lemma 1 which we sketch here:

Lemma. (sketch) Let B denote some integer matrix. There exists an efficient algorithm that computes an SNF matrix B_{SNF} and a number $T \leq 2^{\text{poly}(n)}$ such that

$$\left\| B - \frac{1}{T} B_{SNF} \right\| = 2^{-\tilde{\Omega}(n)},$$

and for any $v \in L(B_{SNF})$, the vector $\hat{v} = B B_{SNF}^{-1} v$ has $\|v/T - \hat{v}\| = O(n^{-k})$, for some fixed k .

1.2 Worst-to-average case lattice reductions

One of the most attractive features of lattice-based crypto-systems is the ability to reduce worst-case instances of such problems to average instances with a small loss in approximation error, thus potentially paving the way to prove that they are one-way functions under standard complexity-theoretic assumptions, namely $\text{NP} \subsetneq \text{BPP}$.

Usually, when speaking of worst-to-average case reductions on lattices, one thinks of a theorem of the following form, as stated in the seminal work of Ajtai [2]

Theorem. (Ajtai) Let $A \in \mathbb{Z}_q^{m \times n}$ be some random matrix, where $q, m = \text{poly}(n)$, and consider $\Lambda(A)^\perp = \{x \in \mathbb{F}_N^n, Ax = 0 \pmod{q}\} \subseteq \mathbb{Z}^n$. If \mathcal{A} is an algorithm that finds a vector $v \in \Lambda(A)^\perp$, $\|v\| \leq \beta \ll q$ with probability at least, say $1/n$, then there exists an algorithm \mathcal{B} such that $\mathcal{B}^{\mathcal{A}}$ can solve gapSVP_γ for $\gamma = \beta \text{poly}(n)$, for any instance, where SVP_γ is the problem of finding a lattice vector which is at most γ longer than the shortest one.

The problem of finding a short vector in $\Lambda(A)^\perp$ is known as the Short-Integer-Solution or SIS, and the statement above means that solving SIS on average is at least as hard as approximating SVP for suitable choice of parameters.

This line of research, pioneered by Ajtai [2], was later improved in the subsequent works of Micciancio and Regev [24], Gentry, Peikert and Vaikuntanathan [17], and Micciancio and Peikert [23]. Specifically, in [24], the authors introduced the use of Gaussian measures, and harmonic (Fourier) analysis on the lattice as a means to simplify the reduction, and achieve better parameters. Most prominently, they reduced the loss in accuracy: i.e. the ratio γ/β , to $O(n\sqrt{\log(n)})$, using a sequence of adaptive reductions.

Essentially, all prior reductions follow the same path, originally due to Ajtai. At a very high level, they amount to querying the SIS oracle in order to iteratively improve (decrease the length) of a set of linearly independent lattice vectors. The oracle is applied to the vector of coefficients of the lattice vectors from previous rounds, which are then shown to be random (modulo \mathbb{Z}_q^m), so long as these vectors are of length which is comparable to the smoothing parameter of the lattice (see Definition 8).

Using the SNF structure, we propose a new worst-to-average case reduction that diverges from the template reduction due to Ajtai. Specifically, we show a simplified scheme that reduces known lattices problem such as Guaranteed-Distance-Decoding (GDD), and Shortest-Independent-Vector-Problem (SIVP) to SIS.

Denote the smoothing parameter of a lattice by $\eta_\varepsilon(L)$ (see Definition 8). We consider the problem of Guaranteed-distance-decoding (GDD) where we are given a lattice $L = L(B)$, and a target vector v , and asked to find a vector $x \in L$, such that $\text{dist}(v, x) \leq \eta_\varepsilon(L)$. We also consider rank-1 instances of the Short-Integer-Solution problem as follows: Fix some prime number N . Given $g = (g_1, \dots, g_n)$, where $g_i \in \mathbb{F}_N$ one can then define a lattice constrained by a “parity” check matrix, as follows:

$$\Lambda(g)^\perp = \{h \in \mathbb{F}_N^n, \langle h, (g_1, \dots, g_n) \rangle = 0 \in \mathbb{F}_N\}.$$

The $\text{SIS}(N)$ problem (see Definition 14), is then to find short vectors in $\Lambda(g)^\perp$, i.e. of length, say $O(n)$. We note that while formally the ensemble above is a proper SIS ensemble, for cryptographic applications one usually uses a completely different range of parameters: the parity check matrix has rank $m = \text{poly}(n)$ (and not 1) and the field of interest is usually taken as $q = \text{poly}(n)$, which is related to the encryption complexity.

We show the following theorem:

Theorem. (sketch) Let (B, v) be an input to GDD where B is an $n \times n$ integer matrix. Suppose that $\eta_\varepsilon(L) \leq \Phi$ for some $\varepsilon = 2^{-n}$. Suppose that \mathcal{A} returns w.p. at least $1/\text{poly}(n)$ a solution to SIS. Then for $x_{\text{out}} = \mathcal{B}(B, v)$ we have that $x_{\text{out}} \in L$ and w.p. $\Omega(1)$

$$\|x_{\text{out}} - v\| \leq \Phi \cdot n^{1.5} \cdot \max\{\log \det(B), n\}.$$

A similar theorem (and algorithm) can be shown for reducing the problem of Shortest-Independent-Vector-Problem (SIVP) to SIS. Following is a sketch of the algorithm:

Algorithm. (sketch)

Input: A lattice $L = L(B)$ for some $n \times n$ HNF matrix B , and vector $v \in \mathbb{F}_N^n$.

1. Reduce L to SNF form. Denote matrix basis by B_{SNF} , matrix M , and constant T . Denote $L_{\text{SNF}} = L(B_{\text{SNF}})$, $N = \det(L_{\text{SNF}})$, $L_N = L_{\text{SNF}} \cap [N]^n$, $NL^* = L(N \cdot B_{\text{SNF}}^{-T})$.
2. Put m as the minimal positive integer for which $\sqrt{m}^m \geq N$. Set $s = T \cdot \eta_\varepsilon(L)$ for some $\varepsilon = O(1)$.
3. Choose c uniformly at random from $\mathbb{F}_N \cap [-m\sqrt{m}, m\sqrt{m}]$. Choose $u_{\text{rand}} \in L_N$ uniformly at random from L_N . Put $v_{\text{target}} = (c^{-1} \cdot T \cdot v + u_{\text{rand}}) \pmod{N}$.
4. Repeat m times:

- (a) Sample $x_i = (x_{i,1}, \dots, x_{i,n}) \sim \rho_{\mathbb{F}_N^n, s, v_{target}}$.
- (b) Compute y_i as the point in NL^* corresponding to x_i . Denote by a_i the first coordinate of y_i .
5. Put $\{\alpha_i\}_{i=1}^m = \mathcal{A}(a_1, \dots, a_m)$.
6. If \mathcal{A} fails or $\sum_{i=1}^m \alpha_i \neq c$ return FAIL.
7. Compute $x_0 = (\sum_{i=1}^m \alpha_i (y_i + x_i) - c u_{rand}) \pmod{N}$.
8. Return $x_{out} := B(B_{SNF}^{-1} M^{-1} \cdot x_0)$.

The algorithm, given target vector t , tries to find a “relatively” close lattice vector to t . This is, in a sense, the same problem as CVP (the closest-vector problem), except here we are only interested in an approximation which is comparable to the “smoothing parameter” of the lattice (see Definitions 11 and 10 for a formal statement). Using Lemma 1, which shows how to reduce an arbitrary lattice to SNF form, and then translate back the solution to the original lattice, we will describe the algorithm assuming the input lattice is already in SNF form.

The reduction begins by sampling from a discrete Gaussian around the target vector t , with sufficiently large variance. Denote these samples by $x_1, \dots, x_n \in \mathbb{F}_N^n$. By the SNF structure, the algorithm then computes for each sampled point x_i , a corresponding point $y_i \in (NL^*)_N$. such that

$$\forall i \quad x_i + y_i \in L_N.$$

We do not know whether such a bijection exists for general lattices.

The structure of the dual lattice implies that the points y_i are completely characterized by their first coordinate. We then show that for sufficiently large Gaussian variance, the first coordinate of these points is uniformly distributed on \mathbb{F}_N^n . This implies that, given as input the first coordinate a_i of each y_i , the random oracle for SIS will succeed with high probability. Suppose that the oracle to SIS returns coefficients $\{\alpha_i\}_{i=1}^m$ such that $\sum_i \alpha_i a_i = 0 \in \mathbb{F}_N$, and consider the linear combination of the vectors x_i using these coefficients:

$$x_0 = \sum_{i=1}^m \alpha_i (x_i + y_i)$$

We note that the above is a lattice point in L_N because it is an integer combination of vectors in L_N . By the SNF structure this implies that $\sum_i \alpha_i y_i = 0$. Hence, the distance of x_0 to the target c is given by the vector:

$$\sum_{i=1}^m \alpha_i x_i = \sum_i \alpha_i t + \sum_{i=1}^m \alpha_i \mathcal{E}_i,$$

where \mathcal{E}_i is a discrete Gaussian on \mathbb{F}_N^n centered around 0 with the same variance as x_i . Since the α_i 's are small (say \sqrt{n}) and the variance of \mathcal{E}_i is s^2 , then to upper bound the length of $x_0 - t$ it is sufficient to make sure that the linear combination of α_i 's is in fact *affine*, i.e. $\sum_{i=1}^m \alpha_i = 1$.

It is not immediately clear why a short-integer-solution to a random instance should be affine. We do know however, that although it may not be affine, the sum of coefficients is quite small, say $O(n\sqrt{n})$. Thus, a natural scheme would be to “guess” the sum of coefficients $c = \sum_{i=1}^m \alpha_i$ in advance out of a small interval, and then sample x_i 's from a Gaussian centered around a scaled target - $\rho_{\mathbb{F}_N^n, s, c^{-1}t}$. For such a scheme to work, we need to rule out the possibility that since we change the original samples to be centered around $c^{-1}t$, the oracle to SIS, despite returning a good answer for almost all inputs, will “adversarially” pick an answer $(\alpha_1, \dots, \alpha_m)$ such that $\sum_{i=1}^m \alpha_i \neq c$ always.

To rule out this possibility, we introduce extra randomization to make sure that the random oracle has no knowledge of which target vector we are looking for. We add a random lattice vector to t , for which we compensate at the end, and then argue that the random oracle can only gain information about the value of t modulo the basic parallelepiped $\mathcal{P}(L)$. But since the x_i 's are sampled with variance above the smoothing parameter, it implies that modulo $\mathcal{P}(L)$ the values of the x_i 's are almost completely uniform.

1.3 Discussion and prior art

The above theorem improves on prior art, and specifically [24] in the following ways:

1. The reduction is direct: in [24] the reduction from GDD to SIS goes through the problem of finding a short linearly independent set called SIVP, and through a variant of GDD called INC – GDD. Hence our reduction is somewhat simpler to follow.
2. It does not rely on the Ajtai form of reductions. Hence it allows to consider other problems as hard random instances: for example, a linear congruence modulo a large prime number N , instead of simultaneous linear equations modulo a small field q [2].
3. It is inherently non-adaptive: the oracle calls to SIS can be made once in parallel, following which the algorithm returns an answer to the original problem (GDD or SIVP).

By [5] it is known that approximating SVP, CVP to a factor at most \sqrt{n} is in $\text{NP} \cap \text{coNP}$, and by [14] and [15] a $\sqrt{n/\log(n)}$ approximation is in $\text{NP} \cap \text{coAM}$. Hence, much larger improvement is needed in order to approach the domain of NP-hardness. In addition, since the reduction is non-adaptive, then by [11] it cannot be used to show a reduction from an NP complete problem to an average case problem, unless the polynomial hierarchy collapses. This suggests, that perhaps an adaptive variant of our algorithm can result a further improvement of the approximation factor.

Finally, we point out that it is not known [27] whether GDD_p is as hard as SVP_q for any polynomials p, q , hence it is possible that approximate GDD (or SIVP) is in fact an *easier* problem than approximate SVP, CVP.

2 Preliminaries

2.1 Notation

The n -dimensional Euclidean space is denoted by \mathbb{R}^n . The Euclidean norm of a vector $x \in \mathbb{R}^n$ is $\|x\| = \sqrt{\sum_{i=1}^n |x_i|^2}$. A Euclidean lattice L is written as $L = L(B)$ where B is some basis of L . N is used to denote a prime number, and \mathbb{F}_N the prime number field corresponding to N . We define Δ as the statistical distance between distributions $(p, \Omega), (q, \Omega)$, i.e. $\Delta(p, q) = \int_{\Omega} |p(x) - q(x)| dx$. Given a set S , $U(S)$ is the uniform distribution on S . For any $v \in \mathbb{R}^n$ define: $|v| = \max_i |v_i|$. For real number $s > 0$ and vector $c \in \mathbb{R}^n$, $\bar{B}_s(c)$ is the closed Euclidean ball of radius s around c . For integer $n \geq 1$, the notation $[n]$ stands for the set of indices $\{1, \dots, n\}$. Given a set $S \subseteq \mathbb{R}^n$, and a vector $v \in \mathbb{R}^n$, we denote $\text{dist}(v, S) := \min_{x \in S} \|v - x\|$. For a positive integer M , we denote by $[M]$ as the interval of integers $[0, \dots, M - 1]$.

We say that a problem P is efficiently computable if there exists an algorithm that runs in time $\text{poly}(n)$, where n is the size of the description of an instance of P .

2.2 Background on lattices

We start by stating some standard facts about lattices.

Definition 1. Euclidean Lattice

A Euclidean lattice $L \subseteq \mathbb{R}^n$ is the set of all integer linear combinations of a set of linearly independent vectors b_1, \dots, b_m :

$$L = \left\{ \sum_{i=1}^m z_i b_i, \quad z_i \in \mathbb{Z}, \right\} \subseteq \mathbb{R}^n$$

This set $\{b_i\}_{i=1}^n$ is called the basis of the lattice. We denote by $L = L(B)$, where B is the matrix whose columns are b_1, \dots, b_m . In this paper, we will always assume that L is full-dimensional, i.e. $m = n$.

For lattice $L = L(B)$, $\mathcal{P}(B)$ is the basic parallelotope of L according to B :

$$\mathcal{P}(B) := \left\{ v = \sum_{i \in [n]} x_i b_i, \ x_i \in [0, 1) \right\}.$$

Sometimes, it will be more convenient to use $\mathcal{P}(L)$ which is independent of the basis. This then refers to $\mathcal{P}(B)$ for some basis B for L .

Definition 2. The Dual Lattice

The dual of a lattice is the lattice generated by the columns of B^{-T} .

Definition 3. Successive minima of a lattice

Given a lattice L of rank n , its successive minima $\lambda_i(L)$ for all $i \in [n]$ are defined as follows:

$$\lambda_i(L) = \inf \{ r \mid \dim(\text{span}(L \cap \bar{B}_r(0))) \geq i \}.$$

Definition 4. Unimodular matrix

The group of unimodular matrices $GL_n(\mathbb{Z})$ is the set of $n \times n$ integer matrices with determinant 1. Unimodular matrices preserve a lattice: $L(B) = L(B')$ if and only if $B = B' \cdot A$, for some unimodular matrix A .

Definition 5. The determinant of a lattice

For a lattice $L = L(B)$ we define $\det(L) = \det(B)$, and denote by N .

The determinant of a lattice is well-defined, since if $L(B') = L(B)$, then by the above $B = B' \cdot A$ for some unimodular matrix A , in which case $\det(B') = \det(B) \det(A) = \det(B)$.

The lattice L is periodic modulo N . In other words, if we add N to any coordinate of a lattice point, we reach another lattice point. Thus, a cube of side length N gives a subset of the lattice which generates the whole lattice when acted on by translations by N in any direction. We let L_N denote the lattice restricted to a cube of side length N .

In particular, if $L = L(B)$ is an integer lattice, with $\det(L) = N$, for prime N , this implies that L_N is a lattice of \mathbb{F}_N^n :

Proposition 1. Let \mathbb{F}_N^n denote the additive group of n -dimensional vectors of integers, where in each coordinate summation is carried out modulo N . Then L_N is an additive sub-group of \mathbb{F}_N^n , that contains the 0 point. In particular L_N is a lattice of \mathbb{F}_N^n .

A canonical representation of integer lattices is called the Hermite normal form (HNF):

Definition 6. Hermite Normal Form

An integer matrix $A \in \mathbb{Z}^{n \times n}$ is said to be in Hermite normal form (HNF) if A is upper-triangular, and $a_{i,i} > a_{i,j} \geq 0$ for all $j > i$, and all $i \in [n]$.

It is well-known that every integer matrix can be efficiently transformed into HNF:

Fact 1. Unique, efficiently-computable, Hermite normal form

For every full-rank integer matrix $A \in \mathbb{Z}^{n \times n}$, there exists a unique unimodular matrix $U \in GL_n(\mathbb{Z})$, such that $H = U \cdot A$, and H is HNF. U can be computed efficiently.

2.3 Gaussians on lattices

The use of the Gaussian measure in the context of lattices is well-known in math. In the context of lattices, the use of the Gaussian measure has been shown in recent years to be very useful to derive important geometric facts about lattices [8] complexity-theoretic results [5], the well-known Learning-with-Errors public-key crypto-system [26], hard random lattices [24] and the fastest classical algorithms for the shortest vector problem [1].

Definition 7. The discrete Gaussian measure over lattices

For any $s > 0$ define the Gaussian function on \mathbb{R}^n centered at c with parameter s :

$$\forall x \in \mathbb{R}^n, \rho_{s,c}(x) = \exp(-\pi\|x - c\|^2/s^2).$$

For any $c \in \mathbb{R}^n$, real number $s > 0$, and n -dimensional lattice L , the discrete Gaussian distribution over L is:

$$\forall x \in L, D_{s,c}(x) = \frac{\rho_{s,c}(x)}{\rho_{s,c}(L)},$$

where

$$\rho_{s,c}(L) = \sum_{x \in L} \rho_{s,c}(x).$$

In [24] Micciancio and Regev introduced a lattice quantity called the smoothing parameter:

Definition 8 (MR07). The smoothing parameter of a lattice

For any n -dimensional lattice and positive real $\varepsilon > 0$, the smoothing parameter $\eta_\varepsilon(L)$ is the smallest real number $s > 0$ for which $\rho_{1/s}(L^* - \{0\}) \leq \varepsilon$.

We mention several important facts by Micciancio, Regev [24]. The first one can be regarded, in a sense as the defining property of the smoothing parameter:

Fact 2. Let L be some integer lattice $L \subseteq \mathbb{R}^n$, $\varepsilon \in (0, 1)$. If $s \geq \eta_\varepsilon(L)$ then for all $c \in \mathbb{F}_N^n$

$$\Delta(D_{\mathbb{F}_N^n, s, c}(\text{mod } \mathcal{P}(L)), U(\mathcal{P}(L))) \leq \varepsilon.$$

The second one states that the smoothing parameter can be chosen arbitrarily close to the n -th minima of the lattice:

Fact 3. For any lattice L , and $\varepsilon = n^{-k}$ for some constant k , we have $\eta_\varepsilon(L) = O(\lambda_n(L) \cdot \sqrt{\log(n)})$.

The third one - is that if we sample from the discrete Gaussian on a lattice L with variance s^2 , then typically a returned vector will have length $s\sqrt{n}$.

Fact 4. For any n -dimensional lattice L , $\varepsilon = o(1)$, real vector $c \in \mathbb{R}^n$, and real number $s \geq \eta_\varepsilon(L)$, we have

$$D_{L, s, c}(L - B_s(c)) = 2^{-\Omega(n)}.$$

2.4 Lattice problems

Definition 9. Closest-vector problem / Shortest-vector problem

The closest-vector problem is defined as follows: Given is a lattice $L = L(B)$, and a vector $v \in \mathbb{R}^n$. Find a lattice vector w for which $\|v - w\| = \text{dist}(v, L)$. The shortest-vector problem is defined as follows: Given $L = L(B)$ find a non-zero lattice vector of minimal length.

Definition 10. Approximate closest-vector (search problem)

The approximate shortest-vector problem CVP_β is the following problem: given a lattice L , and a vector $v \in \mathbb{R}^n$ return $w \in L$ such that $\text{dist}(v, w) \leq \beta \cdot \text{dist}(v, L)$.

Definition 11. Guaranteed-distance decoding - GDD

We are given an n -dimensional integer lattice $L = L(B)$, and $v \in \mathbb{Z}^n$ be some vector. Fix $\varepsilon = \text{poly}(n)$. The problem GDD is to find a vector $w \in L$, such that $\text{dist}(w, v) \leq \eta_\varepsilon(L)$.

The approximate version GDD_γ is to find such a vector $w \in L$ with $\text{dist}(w, v) \leq \eta_\varepsilon(L) \cdot \gamma$.

Definition 12. Shortest Independent Vectors Problem

Let $L = L(B)$ be some n -dimensional lattice. The problem SIVP is to find a set of linearly independent vectors in L , of maximal length at most $\lambda_n(L)$.

The approximate version SIVP_γ is to find such vectors whose length is at most $\lambda_n(L) \cdot \gamma$.

3 The Systematic Normal Form (SNF)

Definition 13. Systematic Normal Form (SNF)

A matrix B is said to be SNF if $B_{i,i} = 1$ for all $i > 1$, and $B_{1,1} = N$ where N is a prime number, and in addition, for all $i > 1$ $B_{i,j} = 0$ for all $i \neq j$.

This form is called suggestively "systematic" because for every $v \in L(B)$, the last $n - 1$ coordinates, are in fact the last $n - 1$ coefficients of the vector under the basis B , which in error-correcting terminology can be considered as the "message" to be encoded by the matrix B .

The following facts will be useful later on:

Proposition 2. If B is in SNF form, then NB^{-T} , i.e. the matrix spanning the scaled dual of $L(B)$ assumes the following form:

$$B = \begin{bmatrix} 1 & & & & \\ -b_2 & 1 & & & \\ -b_3 & & 1 & & \\ \vdots & & & \ddots & \\ -b_n & & & & 1 \end{bmatrix} \quad (3)$$

Proposition 3. There are N^{n-1} points of $L = L(B_{SNF})$ in \mathbb{F}_N^n , and there are N lattice points of NL^* in that cube. Hence there are N points of \mathbb{F}_N^n inside $\mathcal{P}(L)$, and N^{n-1} points in $\mathcal{P}(NL^*)$.

In fact, a somewhat stronger statement is true:

Proposition 4. There exist bijections $\Phi_1 : \mathbb{F}_N^n / L_N \mapsto \mathcal{P}(L)$, $\Phi_2 : \mathcal{P}(L) \mapsto NL^*$ as follows: For every coset of L_N in \mathbb{F}_N^n Φ_1 returns a unique element of $\mathcal{P}(L)$, and Φ_2 maps each element of $\mathcal{P}(L)$ uniquely to an element of $(NL^*)_N = NL^* \cap \mathbb{F}_N^n$ in that coset. Thus, in particular for every $x \in \mathcal{P}(L)$, there exists a unique $z \in (NL^*)_N$, such that $x + z \in L_N$.

Perhaps more interestingly, though, for SNF one can compute efficiently, for each integer vector x , a corresponding dual-lattice vector y , such that their sum is in L_N :

Claim 1. Compute dual vector for any vector

For $x \in \mathbb{F}_N^n$, the map $\Phi_3 := \Phi_2 \circ \Phi_1(x)$ can be computed efficiently.

Proof. Let $x \in \mathbb{F}_N^n$. We would like to find (the unique) $y = \Phi_3(x) = \Phi_2 \circ \Phi_1(x) \in NL^*$ for which $x + y \in L_N$. Each point in $y \in NL^*$ is characterized uniquely by an element $a \in \mathbb{F}_N$ as follows:

$$y = (a, -b_2a(\text{mod } N), \dots, -b_na(\text{mod } N)). \quad (4)$$

Thus, to find y we would like to solve the following vector equality over $a, z_2, \dots, z_n \in \mathbb{F}_N$:

$$(x_1, \dots, x_n)^T + (a, -b_2a(\text{mod } N), \dots, -b_na(\text{mod } N)) = \left(\sum_{i=2}^n b_i z_i(\text{mod } N), z_2, \dots, z_n \right)^T \quad (5)$$

Consider the first coordinate. We have:

$$x_1 + a = \sum_{i=2}^n b_i z_i(\text{mod } N). \quad (6)$$

Substituting in the above $z_i = x_i - ab_i(\text{mod } N)$ for all $i \geq 2$ implies:

$$x_1 - \sum_{i=2}^n x_i b_i = -a \cdot \left(\sum_{i=2}^n b_i^2 + 1 \right) (\text{mod } N). \quad (7)$$

Since N is prime, then the number $\sum_{i=2}^n b_i^2 + 1$ has an inverse. Thus, the parameter a can be computed uniquely from the equation above, which implies that y can be determined uniquely and efficiently. \square

3.1 Reduction to SNF form

In this section we provide an efficient reduction from an arbitrary lattice to a lattice in SNF form, that preserves all important properties of the lattice. Specifically - it allows the reduction of any computational problem on an arbitrary lattice L to another problem on an SNF lattice L_{SNF} such that any solution to the reduced problems allows to find *efficiently* a solution to the problem on L .

Lemma 1. Efficient reduction to SNF

There exists an efficient algorithm that for any LLL-reduced upper-triangular matrix B , and numbers $a > 0, b > 0$, computes efficiently a tuple $\langle B_{SNF}, M, T \rangle$, where B_{SNF} is an SNF matrix, T is a positive integer $T = \max\{2^{O(n)}/\lambda_1(L(B)), \det(B)\}$, and $M \in GL_n(\mathbb{Z})$, such that the following holds: For any $v \in L(B_{snf}/T)$ put $\hat{v} = B \cdot (TB_{snf}^{-1}Mv)$. If $\|v\| \leq \det(B) \cdot n^a$ then $\hat{v} \in L(B)$ and $\|\hat{v} - v\| = O(n^{-b})$. Also $\det(B_{SNF}) = O(\det(B) \cdot T^n)$.

Before presenting the proof, let us bound the coefficients of any short vector in a lattice.

Proposition 5. Let B be an LLL-reduced matrix, and $v \in L$ be some lattice vector. Then v can be represented in the basis B using a vector coefficients of length at most $\|v\| \cdot 2^{O(n)}/\lambda_1(L(B))$.

Proof. Write $v = Bx$, where $x \in \mathbb{Z}^n$. Consider the QR decomposition of B as $B = Q \cdot R$, where Q is a unitary matrix, and R is an upper-triangular matrix. Thus $Q \cdot R$ correspond to the Gram-Schmidt decomposition of B . We express x as:

$$\|x\| = \|B^{-1}v\| \leq \sqrt{n}R_{n,n}^{-1}\|v\|, \quad (8)$$

where the second inequality follows from unitarity of Q . By LLL we know that for some constant $\beta > 0$ we have:

$$\lambda_1 := \lambda_1(L) \leq R_{1,1} \leq 2^{\beta n} \cdot R_{n,n}. \quad (9)$$

Therefore

$$R_{n,n} \geq 2^{-\beta n} \lambda_1. \quad (10)$$

This implies that

$$\|x\| \leq \sqrt{n}R_{n,n}^{-1}\|v\| \leq \|v\|\sqrt{n} \cdot 2^n / \lambda_1 = \|v\| \cdot 2^{O(n)} / \lambda_1. \quad (11)$$

□

The following are easy corollaries of the above:

Proposition 6. Let $B_1 = \{v_i\}_{i=1}^n$ be some LLL-reduced basis and another basis $B_2 = \{w_i\}_{i=1}^n$ for lattice $L_2 = L(B_2)$. Suppose that $\|v_i - w_i\| \leq \alpha$. Let $v = \sum_{i=1}^n c_i v_i$ be a point in L_1 and $w = \sum_{i=1}^n c_i w_i$ be the corresponding point in L_2 . Then $\|v - w\| \leq \|v\| \alpha 2^{O(n)} / \lambda_1(L_1)$.

Proof. By the triangle inequality we have:

$$\|v - w\| = \left\| \sum_{i=1}^n c_i v_i - \sum_{i=1}^n c_i w_i \right\| \quad (12)$$

$$\leq \sum_{i=1}^n \|v_i - w_i\| |c_i| \quad (13)$$

$$\leq n\alpha \|v\| \cdot 2^{O(n)} / \lambda_1(L_1) \quad (14)$$

$$= \alpha \|v\| \cdot 2^{O(n)} / \lambda_1(L_1), \quad (15)$$

where the inequality before last follows from Proposition 5. □

3.2 Proof of Lemma 1

Proof. We first use T as a parameter and determine it later on in the proof. We start from an upper-triangular LLL-reduced matrix B_1 :

$$B_1 = \begin{bmatrix} b_{1,1} & b_{1,2} & b_{1,3} & \dots & b_{1,n} \\ & b_{2,2} & b_{2,3} & \dots & b_{2,n} \\ & & b_{3,3} & \dots & b_{3,n} \\ & & & \ddots & \vdots \\ & & & & b_{n,n} \end{bmatrix} \quad (16)$$

add $1/T$ along the subdiagonal, and truncate each non-zero entry to its nearest integer multiple of $1/T$:

$$B_2 = \begin{bmatrix} b'_{1,1} & b'_{1,2} & b'_{1,3} & \dots & b'_{1,n} \\ \frac{1}{T} & b'_{2,2} & b'_{2,3} & \dots & b'_{2,n} \\ & \frac{1}{T} & b'_{3,3} & \dots & b'_{3,n} \\ & & \ddots & \ddots & \vdots \\ & & & \frac{1}{T} & b'_{n,n} \end{bmatrix}, \quad (17)$$

where $b'_{i,j} = \lfloor b_{i,j}T \rfloor / T$. We note that

$$\forall i, j \quad |B_2(i, j) - B_1(i, j)| \leq 1/T. \quad (18)$$

We now use column operations to make rows 2, 3, ..., n of the lattice zero except for the subdiagonal. This involves subtracting integer multiples of the i th column from all later columns. We obtain a lattice of the form.

$$B_3 = \begin{bmatrix} b'_{1,1} & b''_{1,2} & b''_{1,3} & \dots & b''_{1,n} \\ \frac{1}{T} & 0 & 0 & \dots & 0 \\ & \frac{1}{T} & 0 & \dots & 0 \\ & & \ddots & \ddots & \vdots \\ & & & \frac{1}{T} & 0 \end{bmatrix} \quad (19)$$

Observe that if we move the n th column to the first column and multiply all entries by T , we now have a lattice which is a $1/T$ multiple of an SNF lattice, except possibly from the entry $b''_{1,n}$ which may not be prime.

We now show how to make determinant of the new lattice prime, by rounding $b''_{1,n}$ to a prime. By standard number-theory conjecture¹ we assume:

$$\exists \delta = O(\log(Tb''_{1,n})), \quad Tb''_{1,n} + \delta \text{ is prime.} \quad (20)$$

We need to compute the matrix that transforms the basis given in equation (17) to the basis given in equation (19). That is, we want the matrix M such that $B_3 = B_2M$. The diagonal and

¹Generalized Riemann Hypothesis (GRH)

superdiagonal of the matrix can be easily calculated:

$$M = \begin{pmatrix} 1 & Tb'_{2,2} & Tb'_{2,3} & \dots & Tb'_{2,n-1} & Tb'_{2,n} \\ & 1 & Tb'_{3,3} & \dots & Tb'_{3,n-1} & Tb'_{3,n} \\ & & 1 & \dots & Tb'_{4,n-1} & Tb'_{4,n} \\ & & & \ddots & \vdots & \vdots \\ & & & & 1 & Tb'_{n,n} \\ & & & & & 1 \end{pmatrix}^{-1} \quad (21)$$

$$= \begin{pmatrix} 1 & -Tb'_{2,2} & \dots & \dots & \dots & \dots \\ & 1 & -Tb'_{3,3} & \dots & \dots & \dots \\ & & 1 & -Tb'_{4,4} & \dots & \dots \\ & & & \ddots & \ddots & \vdots \\ & & & & 1 & -Tb'_{n,n} \\ & & & & & 1 \end{pmatrix} \quad (22)$$

By the above, M is a unimodular matrix, hence $\det(B_2) = \det(B_3)$. Note that both M and M^{-1} are upper triangular matrices with 1s along the diagonal. The determinant of TB_3 is $Tb'_{1,n}$. To obtain a lattice with a prime determinant, we need to round $\det(TB_3)$ to a nearby prime. Let us assume that $\det TB_3 + \delta$ is prime. This rounding corresponds to adding δ/T to the entry $B_3(1, n)$.

What effect does this change have on the basis of the lattice in B_2 ? Let Δ be the matrix with $\Delta(1, n) = \delta/T$ and all other entries 0. Then our matrix in the SNF basis is $B_3 + \Delta$. To see what the effect on B_2 is, we merely need to multiply by M^{-1} . That is,

$$B_2 + \Delta M^{-1} = (B_3 + \Delta)M^{-1}. \quad (23)$$

Using the form we derived above for M^{-1} , we see that because there are 1s along the diagonal of M then $\Delta M^{-1} = \Delta$. Thus, we can make B_2 obtain a prime determinant by simply adding δ/T to $B_2(1, n) = b'_{1,n}$. This changes the length of the n th basis vector by at most δ/T .

Let B_4 denote then the output SNF matrix.

$$B_4 = \begin{bmatrix} Tb''_{1,n} + \delta & Tb'_{1,1} & Tb'_{1,2} & \dots & Tb'_{1,n-1} \\ 0 & 1 & 0 & \dots & 0 \\ & 0 & 1 & \dots & 0 \\ & & \ddots & \ddots & \vdots \\ & & & 0 & 1 \end{bmatrix} \quad (24)$$

By Equations 18 and equation 20 :

$$\forall i, j \in [n] |(M^{-1}B_4(i, j))/T - B_1| = O(\log(Tb''_{1,n})/T). \quad (25)$$

That is, the basis $M^{-1}B_4/T$ of $L(B_4)/T$ is entry-wise close to B_1 . By assumption B_1 is in particular LLL-reduced. Hence we can invoke Proposition 6 w.r.t. these two bases: Consider some $v \in L(B_4/T)$. Let β denote the implicit constant in the bound of Proposition 6. Applying Proposition 6 implies that the corresponding vector $\hat{v} = B_1 \cdot (TB_4^{-1}M) \cdot v \in L(B_1)$ has

$$\|\hat{v} - v\| \leq \frac{2^{\beta n} \|v\| \log(Tb''_{1,n})}{T \lambda_1(L(B_1))}. \quad (26)$$

By assumption $\|v\| \leq n^a \det(B_1)$. Then together with Equation 26 we conclude that there exists

$$T = \text{poly}(n) \cdot \max\{\det(B_1)/\lambda_1(L(B_1)), 2^{\beta n}\}. \quad (27)$$

such that

$$\|\hat{v} - v\| \leq n^{-b}. \quad (28)$$

Finally, the entry $B_{SNF}(1, 1) = \det(B_{SNF}) \leq 2b'_{1,n} \cdot T^n$, hence the determinant $\det(B_{SNF})$ is upper-bounded by

$$\det(B_{SNF}) = O(\det(B)T^n). \quad (29)$$

□

The lemma above implies that one can reduce the standard lattice problems, given for an arbitrary lattice, to the same problem on a lattice in SNF, and then translate the output solution efficiently to a solution for the original lattice:

Corollary 1. SNF reduction preserves approximate CVP

Let (B, v) be an input to CVP_γ for some γ , where B is an LLL-reduced upper-triangular matrix. Let $\langle B_{SNF}, T, M \rangle$ denote the tuple returned by the SNF reduction, for parameters $a > 1/2, b$. Suppose that for $x_0 \in L(B_{SNF})$, $v \in [\det(B)]^n \cap \mathbb{Z}^n$ we have $\|x_0 - Tv\| \leq \gamma \cdot \text{dist}(Tv, L(B_{SNF}))$, for $\gamma = n^{a-1/2}$. Then the vector $x_{out} := B(B_{SNF}^{-1}M)x_0 \in L(B)$ has

$$\|x_{out} - v\| \leq \gamma \cdot \text{dist}(v, L(B)).$$

Proof. Denote $L = L(B)$, $L_{SNF} = L(B_{SNF})$. By the triangle inequality:

$$\|x_{out} - v\| = \|x_{out} - x_0/T + x_0/T - v\| \leq \|x_0/T - v\| + \|x_0/T - x_{out}\| \quad (30)$$

Since

$$x_0 \in L_{SNF} \text{ and } \|x_0 - Tv\| \leq \gamma \cdot \text{dist}(Tv, L_{SNF}) \quad (31)$$

then together with the above we have that $x_{out} \in L$ and

$$\|x_{out} - v\| \leq \frac{1}{T} \|x_0 - Tv\| + \|x_0/T - x_{out}\| \quad (32)$$

$$\leq \frac{1}{T} \gamma \cdot \text{dist}(Tv, L_{SNF}) + \|x_0/T - x_{out}\| \quad (33)$$

$$\leq \gamma \cdot \text{dist}(v, L) + \|x_0/T - x_{out}\|, \quad (34)$$

where in the last inequality we used again Lemma 1. Since v is an integer vector, we can assume that the length of x_0 is bounded by:

$$\|x_0\| \leq \gamma \|Tv\| = \gamma T \|v\|, \quad (35)$$

hence

$$\|x_0/T\| \leq \gamma \|v\| \leq \gamma \det(B) \sqrt{n} = n^a \det(B). \quad (36)$$

By assumption $x_0 \in L_{SNF}$ so $x_0/T \in L(B_{SNF}/T)$. Hence, by Lemma 1 and together with the above equation 36 then $x_{out} \in L(B)$ and we have

$$\|x_{out} - x_0/T\| = O(n^{-b}). \quad (37)$$

Plugging this inequality into Equation 34 implies the proof.

□

3.3 Uniform distribution on SNF-dual

Fact 5. Let $L \subseteq \mathbb{F}_N^n$ be some SNF lattice, $\det(L) = N$, and let \mathcal{D}^* denote the distribution on NL^* defined by sampling $x \sim D_{\mathbb{F}_N^n, s, c}$, and computing the corresponding element $y \in (NL^*)_N = \Phi_3(x)$. If $s \geq \eta_\varepsilon(L)$ then $\Delta(\mathcal{D}^*, U[(NL^*)_N]) \leq \varepsilon$.

Proof. By Fact 2 we have $\Delta((D_{\mathbb{F}_N^n, s, c} \bmod \mathcal{P}(L)), U(\mathcal{P}(L))) \leq \varepsilon$. By Proposition 4 Φ_3 is a bijection between $\mathcal{P}(L)$ and $(NL^*)_N$, so therefore: sampling $x \sim \rho_{\mathbb{F}_N^n, s, c}$, and computing $y = y(x) \in (NL^*)_N$ results in a distribution D^* which is ε close to $U[(NL^*)_N]$. \square

4 Rank-1 SIS with Prime Modulus

In this work we will use a somewhat different variant of the Ajtai ensemble that arises naturally from the SNF reduction. We define formally our variant of SIS as follows:

Definition 14. Short-Integer-Solution $\text{SIS}(N, \delta)$ - homogeneous

Let N be some prime number, and $\delta > 0$ some constant. Fix n as the minimal positive integer for which $N \leq n^{\delta n}$. Given are n numbers $g_1, \dots, g_n \in \mathbb{F}_N$. The Short-Integer-Solution problem is to find n numbers $h_1, \dots, h_n \in \mathbb{F}_N$, such that

$$\sum_{i=1}^n h_i g_i = 0 \in \mathbb{F}_N, \text{ and } \max_{i=1}^n |h_i| \leq 2n^\delta.$$

Alternatively, $\text{SIS}(N)$ asks for a short vector in the lattice

$$L = L(g)^\perp := \{h \in \mathbb{F}_N^n, \langle (g_1, \dots, g_n), h \rangle = 0 \in \mathbb{F}_N\}.$$

We note [29] that one can formulate $\text{SIS}(N)$ also as a non-homogeneous congruence of the following form

Definition 15. Short-Integer-Solution $\text{SIS}(N, \delta)$ - non-homogeneous

Let N be some prime number, and $\delta > 0$ some constant. Fix n as the minimal positive integer for which $N \leq n^{\delta n}$. Given are n numbers $g_1, \dots, g_n \in \mathbb{F}_N$. The Short-Integer-Solution problem is to find $n + 1$ numbers $h_0, h_1, \dots, h_n \in \mathbb{F}_N$, such that

$$\sum_{i=1}^n h_i g_i = h_0 \in \mathbb{F}_N, \text{ and } \max_{i=0}^n |h_i| \leq 2n^\delta.$$

Similarly to the homogeneous case we can define $\text{SIS}(N)$ as asking for short vectors in the following $n + 1$ -dimensional lattice:

$$L = L(g)_1^\perp := \{h \in \mathbb{F}_N^{n+1}, \langle (1, g_1, \dots, g_n), h \rangle = 0 \in \mathbb{F}_N\}.$$

To see why the two problems are equivalent, note that we can implement an oracle \mathcal{O}_h for the homogeneous $\text{SIS}(N, \delta)$ using oracle calls to \mathcal{O}_n for the non-homogeneous $\text{SIS}(N, \delta/2)$ as follows: Given g , call $\mathcal{O}_n(g) = \{h_i\}_{i=0}^n$, i.e.

$$\sum_i h_i g_i = h_0 \pmod{N}.$$

Then call

$$\mathcal{O}_n(h_0^{-1}g) = \{h'_i\}_{i=0}^n.$$

Then by definition

$$\sum_{i=1}^n h'_i h_0^{-1} g_i = h'_0$$

so

$$\sum_{i=1}^n h'_i g_i = h_0 h'_0 = h'_0 \sum_{i=1}^n h_i g_i,$$

which implies that

$$\sum_{i=1}^n (h'_i - h'_0 h_i) g_i = 0 \pmod{N},$$

and since $|h_i|, |h'_i|$ are bounded by $n^{\delta/2}$ for all i this implies that $\{h'_i - h'_0 h_i\}_{i=1}^n$ are bounded by $n^{\delta/2} + n^{\delta/2} n^{\delta/2} \leq 2n^\delta$, hence it is a valid solution to $\mathcal{O}_h(g)$.

The significance of the non-homogeneous version is evident in the following equivalence of definitions:

Proposition 7. *Let B be an SNF matrix, with $\det(B) = N$. Then $L(B) = L(g)_\perp^\perp$ where g is the $n-1$ -dimensional vector $g = (b_2, \dots, b_n)$.*

The random - approximate SIS problem (rSIS(N)) is then defined by having g_1, \dots, g_n be chosen independently and uniformly at random. We also define an approximation variant called SIS $_\gamma$ in which the solution $\{h_i\}$ must satisfy $\max_i |h_i| \leq n^\delta \gamma$. As in previous works, one can establish the existence of a solution to the SIS problem for any input, using the pigeonhole principle:

Fact 6. *For any N, δ the (homogeneous / non-homogeneous) SIS(N, δ) problem has a solution.*

Proof. Fix some $h_0 \in \mathbb{F}_N$. By definition, there are at least $n^{\delta n}$ vectors of coefficients (h_1, \dots, h_n) whose magnitude is at most n^δ . Since $N \leq n^{\delta n}$ there are at least two n -dimensional coefficient vectors $h \neq h'$ for which $\sum_{i=1}^n h_i g_i = \sum_{i=1}^n h'_i g_i = h_0 \pmod{N}$. Hence the vector $(h_1 - h'_1, \dots, h_n - h'_n)$ is a non-zero n -dimensional vector which is a valid solution. \square

Next, we adapt an argument that appeared in [4] which discussed the Ajtai ensemble of lattices, for our ensemble of random lattices - rSIS(N):

Lemma 2. Random SIS lattices are dense

Let N be some prime number, $\delta \leq 1/2$, and consider the lattice defined by SIS(N, δ), for some numbers $g_1, \dots, g_n \in \mathbb{F}_N$:

$$L = L(g)^\perp := \{z \in \mathbb{Z}^n, \langle (g_1, \dots, g_n), z \rangle = 0\}.$$

With high probability when choosing the numbers $\{g_i\}_{i=1}^n$ independently and uniformly at random from \mathbb{F}_N we have that $\lambda_i(L(g)^\perp) = \Theta(\sqrt{n})$ for all $i \in [n]$.

Proof. By definition n is the minimal positive integer for which $N \leq n^{\delta n}$. There exists such n for which $N \geq n^{\delta(n-1)}$.² The argument has two parts: First, is that $\det(L) \leq N$ - this is immediate because there are at most N congruence classes of \mathbb{Z}^n/L by definition. Next, for any integer n and constant α let:

$$N_{\alpha, n} = |\{z \in \mathbb{F}_N^n, \|z\| \leq \alpha\sqrt{n}\}|. \quad (38)$$

By [25] for every ε , there exists an α such that $N_{\alpha, n} \leq \varepsilon^n$. Fix a vector $v \in N_{\alpha, n}$. We have that $\mathbb{P}_{g \sim U[\mathbb{F}_N^n]}(v \in L(g)^\perp) = 1/N$. Hence by the union bound

$$\mathbb{P}(\{z \in \mathbb{F}_N^n, \|z\| \leq n^\delta\} \cap L(g)^\perp \neq \emptyset) \leq \varepsilon^n / N \leq \varepsilon^n / n^{\delta(n-1)} < 1. \quad (39)$$

Together with the assumption $\delta \leq 1/2$ this implies that w.p. $1 - O(1)$ we get $\lambda_1(L(g)^\perp) \geq \alpha n^\delta$. This implies by definition that $\lambda_i(L) \geq \alpha n^\delta$ for all $i \in [n]$. Together with the fact that $\det(L) \leq N \leq n^{\delta n}$, it implies that $\lambda_i(L) = \Theta(n^\delta)$ for all $i \in [n]$. \square

²assuming Bertrand-Chebyshev theorem, and sufficiently large n .

5 Reduction from worst-case GDD to random SIS

In this section we show a reduction from a variant of CVP called Guaranteed-Distance-Decoding, or GDD, (see Definition 11) to random SIS. Let \mathcal{A} denote an algorithm for $\text{SIS}(N)$. We define the following algorithm:

Algorithm. \mathcal{B}

Input: An integer matrix B , and vector $v \in \mathbb{Z}^n$, and parameter $\delta > 0$.

1. Reduce B via LLL, denote by B_{LLL} .
2. Decompose B_{LLL} by QR decomposition, $B_{LLL} = Q \cdot R$, set $\hat{v} = Q^\dagger v$.
3. Reduce R to SNF form: $\langle B_{SNF}, M, T \rangle$. Denote $L_{SNF} = L(B_{SNF})$, $N = \det(L_{SNF})$, $L_N = L_{SNF} \cap \mathbb{F}_N^n$, $NL^* = L(N \cdot B_{SNF}^{-T})$.
4. Put m as the minimal positive integer for which $m^{\delta m} \geq N$. Let Φ denote the minimal number for which: $\eta_\varepsilon(L) \leq \Phi$ for $\varepsilon = m^{-5}$. Set $s = T \cdot \Phi$.
5. Choose c uniformly at random from $\mathbb{F}_N \cap [-m^{1+\delta}, m^{1+\delta}]$. Choose $u_{rand} \in L_N$ uniformly at random from L_N . Put $v_{target} = (c^{-1} \cdot T \cdot \hat{v} + u_{rand}) \pmod{N}$.
6. Repeat m times:
 - (a) Sample $x_i = (x_{i,1}, \dots, x_{i,n}) \sim D_{\mathbb{F}_N^n, s, v_{target}}$.
 - (b) Compute $y_i = \Phi_3(x_i)$. Denote by a_i the first coordinate of y_i .
7. Put $\{\alpha_i\}_{i=1}^m = \mathcal{A}(a_1, \dots, a_m)$.
8. If \mathcal{A} fails or $\sum_{i=1}^m \alpha_i \neq c$ return FAIL.
9. Compute $x_0 = \sum_{i=1}^m \alpha_i(y_i + x_i) - cu_{rand} \pmod{N}$.
10. Return $x_{out} := Q \cdot R \cdot (B_{SNF}^{-1} M^{-1} \cdot x_0)$.

The theorem below is stated so that for an oracle \mathcal{A} that returns a correct answer w.p. $1-o(1)$ the algorithm \mathcal{B} computes the correct answer w.p. $1/\text{poly}(n)$. However, by making multiple (parallel) calls to the oracle \mathcal{A} , and algorithm \mathcal{B} , the probability of success can be amplified to an arbitrary constant, while using an oracle that returns a correct answer w.p. $1/\text{poly}(n)$. We note that by Lemma 1, the minimal m for which $m^{\delta m} \geq N$, where $N = \det(B_{SNF})$ is polynomial in n , i.e. $m = \text{poly}(n)$. Thus, for simplicity, in our main theorem we state the probability of success as a function of m instead of n .

Theorem 1. *Let (B, v) be an input to GDD where B is an $n \times n$ integer. Suppose that \mathcal{A} returns w.p. at least $1 - m^{-3}$ a solution to $\text{SIS}(N, \delta)$. Then for $x_{out} = \mathcal{B}(B, v)$ we have $x_{out} \in L$ and w.p. $\Omega(m^{-2})$ we have:*

$$\|x_{out} - v\| \leq \Phi \cdot \text{dist}(v, L) \cdot O(n^{1.5+\delta} \cdot \max\{n, \log \det(B)\}^{1+\delta}).$$

Proof. B_{LLL} is LLL-reduced, hence the matrix R as a basis for $L = L(R)$ is trivially also LLL-reduced. R is thus LLL-reduced and upper-triangular which means we can invoke Lemma 1 w.r.t. R , and derive the tuple $\langle B_{SNF}, M, T \rangle$ which has the properties of the lemma. In particular, by Corollary 1 if

$$(\star) \quad x_0 \in L_{SNF} \text{ and } \|x_0 - T\hat{v}\| \leq \gamma \cdot T\Phi \tag{40}$$

then

$$R \cdot (B_{SNF}^{-1} M^{-1} \cdot x_0) \in L(R) \text{ and } \|R \cdot (B_{SNF}^{-1} M^{-1} \cdot x_0) - \hat{v}\| \leq \gamma\Phi + O(n^{-k}), \tag{41}$$

and since Q is a unitary matrix then

$$x_{out} \in L(B), \quad \|x_{out} - v\| = \|R \cdot (B_{SNF}^{-1} M^{-1} \cdot x_0) - \hat{v}\| \leq \gamma\Phi + O(n^{-k}). \tag{42}$$

We will first show that when \mathcal{B} terminates then the output vector has property (\star) . Then, we will show that \mathcal{B} succeeds with high probability.

Property (★) - quality of estimate:

By Claim 1 we have:

$$\forall i \in [m], \quad x_i + \Phi_3(x_i) = x_i + y_i \in L. \quad (43)$$

Since $x_i \sim D_{\mathbb{F}_N^n, s, v_{target}}$, for $v_{target} \in \mathbb{F}_N^n$ we can write

$$x_i = c^{-1}T\hat{v} + u_{rand} + \mathcal{E}_i, \quad \mathcal{E}_i \sim D_{\mathbb{F}_N^n, s, 0}. \quad (44)$$

Since we choose m such that $N \leq \sqrt{m}^m$ then by Fact 6 there exists a short solution, i.e. whenever \mathcal{A} succeeds it returns a set of coefficients $\alpha_1, \dots, \alpha_m$, $|\alpha_i| \leq \beta\sqrt{m}$, for some constant β , and in addition

$$\sum_{i=1}^m \alpha_i a_i = 0.$$

Assume from now on that this is the case. Using again Equation 4 implies that

$$\sum_{i=1}^m \alpha_i y_i = 0 \in \mathbb{F}_N, \quad |\alpha_i| \leq \beta m^\delta, \quad \forall 1 \leq i \leq n \quad (45)$$

Now, assume that $\sum_{i=1}^m \alpha_i = c$, in which case the algorithm \mathcal{B} declares success and consider the vector:

$$x_0 := \sum_{i=1}^m \alpha_i (x_i + y_i) - cu_{rand}. \quad (46)$$

On one hand: by definition $x_0 \in L_{SNF}$, because the α_i 's and c are integers, $u_{rand} \in L_N$, and by Equation 43 $x_i + y_i \in L_N$ for all i . On the other hand by Equation 44

$$T\hat{v} - x_0 = T\hat{v} - \sum_{i=1}^m \alpha_i y_i - \sum_{i=1}^m \alpha_i (c^{-1}T\hat{v} + u_{rand}) - \sum_{i=1}^m \alpha_i \mathcal{E}_i + cu_{rand} \quad (47)$$

In addition, by the assumption that $\sum_{i=1}^m \alpha_i = c$ we get:

$$\sum_{i=1}^m \alpha_i c^{-1}T\hat{v} = T\hat{v}c^{-1} \cdot \sum_{i=1}^m \alpha_i = T\hat{v} \cdot c^{-1} \cdot c = T\hat{v}, \quad (48)$$

and similarly

$$\sum_{i=1}^m \alpha_i u_{rand} = cu_{rand}. \quad (49)$$

Hence

$$T\hat{v} - x_0 = \sum_i \alpha_i \mathcal{E}_i \quad (50)$$

By Equation 44 $\mathcal{E}_i \sim D_{\mathbb{F}_N^n, s, 0}$ for all i , so by Fact 4

$$\forall i, \quad \mathbb{P}(\|\mathcal{E}_i\| \leq s\sqrt{n}) = 1 - 2^{-\Omega(n)}, \quad (51)$$

and so by the union bound:

$$\mathbb{P}(\forall i, \|\mathcal{E}_i\| \leq s\sqrt{n}) = 1 - 2^{-\Omega(n)} = 1 - o(1). \quad (52)$$

Next, by Equation 45 the random variables α_i are bounded by m^δ hence

$$\mathbb{P}(\|T\hat{v} - x_0\| \leq s \cdot m^{1+\delta} \cdot \sqrt{n}) = 1 - o(1). \quad (53)$$

We note that in the above we assume a worst-case scenario where the summation $\sum_i \alpha_i \mathcal{E}_i$ is coherent, i.e. the α_i 's are completely correlated with the \mathcal{E}_i 's. Together with our choice $s = T\Phi$ this implies that

$$\mathbb{P}(\|T\hat{v} - x_0\| \leq T\phi m^{1+\delta}\sqrt{n}) = 1 - o(1). \quad (54)$$

Since m is the minimal integer for which $m^{\delta m} \geq N$ then by Bertrand-Chebyshev theorem for sufficiently large m we have:

$$m^{\delta(m-1)} \leq N. \quad (55)$$

In addition, by Lemma 1 we have $T \leq \max\{\det(B), 2^{O(n)}\}$ and $N = O(\det(B)T^n)$. Hence $m = O(n \max\{n, \log \det(B)\})$. Thus, w.p. $1 - o(1)$ we have

$$\|T\hat{v} - x_0\| = O(n^{1.5+\delta}T\Phi \max\{n, \log \det(B)\}^{1+\delta}), \quad (56)$$

in which case by Equation 41

$$\|v - x_{out}\| = \Phi \cdot O(n^{1.5+\delta} \max\{n, \log \det(B)\}^{1+\delta}). \quad (57)$$

Probability of success:

Now we would like to lower-bound the probability of the algorithm succeeding. By our choice of $s = T \cdot \eta_\varepsilon(L)$, and Lemma 1 we have: $s \geq \eta_\varepsilon(L_{SNF})$. Hence, by Fact 5 we have that

$$\Delta(y_i, U[(NL^*)_N]) \leq \varepsilon. \quad (58)$$

By equation 4 this implies that $\Delta(a_i, U[N]) \leq \varepsilon$, and since the a_i 's are independent then

$$\Delta((a_1, \dots, a_m), U[N^m]) \leq 1 - (1 - \varepsilon)^m \leq m^{-3}, \quad (59)$$

where the last inequality follows from our choice of $\varepsilon = m^{-5}$. By assumption, algorithm \mathcal{A} for $\text{SIS}(N)$ returns a correct answer w.p at least $1 - m^{-3}$, for a uniformly random vector (a_1, \dots, a_m) . Therefore

$$\mathbb{P}(\mathcal{A} \text{ succeeds}) \geq 1 - m^{-3} - m^{-3} = 1 - O(m^{-3}). \quad (60)$$

Next, we would like to make sure that \mathcal{A} is not "adversarial", and given c , returns $\alpha_1, \dots, \alpha_m$ whose sum is different than c almost all the time. Using Fact 7, for any $c_1, c_2 \in [N]$ we have:

$$\Delta(\mathbb{P}(\alpha_1, \dots, \alpha_m | c_1), \mathbb{P}(\alpha_1, \dots, \alpha_m | c_2)) \leq m^{-3}. \quad (61)$$

Hence, given a choice of c by the algorithm, the probability that the same c is going to be the value of $\sum_i \alpha_i$ is lower-bounded by:

$$\mathbb{P}\left(\sum_{i=1}^m \alpha_i = c | c\right) \geq \max_{c'} \mathbb{P}\left(\sum_i \alpha_i = c'\right) - m^{-3} = \Omega\left(\frac{1}{m^{1+\delta}}\right), \quad (62)$$

where the inequality follows because $|\alpha_i| \leq 2m^\delta$ for each i , and so $|\sum_i \alpha_i| \leq 2m^{1+\delta}$. By the union bound we thus have:

$$\mathbb{P}(\mathcal{B} \text{ succeeds}) = \mathbb{P}\left(\mathcal{A} \text{ succeeds} \wedge \sum_{i=1}^m \alpha_i = c\right) = \Omega(m^{-1-\delta}) - O(m^{-3}) = \Omega(m^{-2}). \quad (63)$$

□

Fact 7. For any $c_1, c_2 \in [N]$:

$$\Delta(\mathbb{P}(\alpha_1, \dots, \alpha_m | c_1), \mathbb{P}(\alpha_1, \dots, \alpha_m | c_2)) \leq m^{-3}.$$

Proof. Since y_i is uniquely determined from x_i for each i , and $(\alpha_1, \dots, \alpha_m)$ is determined (possibly probabilistically) from the pairs (y_i, x_i) for all $i \in [n]$ then it is sufficient to show that for any $c_1 \neq c_2$, we have

$$\Delta(P(x_1, \dots, x_m|c_1), P(x_1, \dots, x_m|c_2)) \leq m^{-3}. \quad (64)$$

By definition, we have:

$$P(x_1, \dots, x_m|c) \propto \prod_{i=1}^m e^{-\pi \|x_i - vc - u_{rand}\|^2 / s^2}. \quad (65)$$

Since u_{rand} is uniform on L_N , and chosen independently of c , then it is sufficient to consider the a-posteriori probabilities of the vectors x_i modulo $\mathcal{P}(L)$ for each i :

$$P(x_1^L, \dots, x_m^L|c), \quad x_i^L := x_i \bmod \mathcal{P}(L). \quad (66)$$

Finally, since the x_i 's are independent given c then:

$$P(x_1^L, \dots, x_m^L|c) = \prod_{i=1}^m P(x_i^L|c) \quad (67)$$

Hence, for $c_1 \neq c_2$ we have:

$$\Delta(P(x_1, \dots, x_m|c_1), P(x_1, \dots, x_m|c_2)) = \Delta\left(\prod_{i=1}^m P(x_i^L|c_1), \prod_{i=1}^m P(x_i^L|c_2)\right). \quad (68)$$

Since $s \geq \eta_\varepsilon(L_{SNF})$ then by Fact 2 and the triangle inequality we have:

$$\forall i \in [m] \quad \Delta(P(x_i^L|c_1), P(x_i^L|c_2)) \leq 2\varepsilon \quad (69)$$

which implies by Equation 68

$$\Delta(P(x_1, \dots, x_m|c_1), P(x_1, \dots, x_m|c_2)) \leq 1 - (1 - 2\varepsilon)^m = O(m^{-4}), \quad (70)$$

where the last equality follows from our choice $\varepsilon = m^{-5}$. \square

We note that by a simple modification of the algorithm above one can obtain a reduction from approximate SIVP to rSIS(N):

Theorem 2. *Given is an integer matrix B . Let Φ denote the number defined by: $\eta_\varepsilon(L) \leq \Phi$ for $\varepsilon = m^{-5}$. Suppose that \mathcal{A} returns w.p. at least $1 - m^{-3}$ a solution to rSIS(N, δ). There exists an algorithm \mathcal{B} such that $\mathcal{B}^{\mathcal{A}}$ returns w.p. $1 - o(1)$ a vector $x_{out} \in L$, such that*

$$\|x_{out}\| \leq \Phi \cdot O(n^{1.5+\delta} \max\{n, \log \det(B)\}^{1+\delta}).$$

Proof. We slightly modify algorithm \mathcal{B} as follows: we set $v_{target} = u_{rand} = v = 0$ in step (3). In Step (6) we terminate successfully whenever \mathcal{A} succeeds (i.e. regardless of the sum of coefficients). Similar to Equation 57 we have:

$$x_{out} \in L, P(\|x_{out}\| \leq \Phi \cdot O(n^{1.5+\delta} \max\{n, \log \det(B)\}^{1+\delta})) = 1 - o(1). \quad (71)$$

Hence, sampling n such vectors x_{out} independently returns w.h.p. a set of n linearly-independent vectors, with the desired approximation ratio. \square

6 Acknowledgements

The authors are thankful to Oded Regev and Vinod Vaikuntanathan for their important insights regarding SIS and to the following people for useful discussion and insightful comments: Shafi Goldwasser, Sean Hallgren, David Jerison, Daniele Micciancio, Noah Stephens-Davidowitz. LE is thankful to the Templeton foundation for their support of this work. PWS was supported by the US Army Research Laboratory's Army Research Office through grant number W911NF-12-1-0486, the NSF through grant number CCF-121-8176, and by the NSF through the STC for Science of Information under grant number CCF0-939370.

References

- [1] D. Aggarwal, D. Dadush, O. Regev, N. Stephens-Davidowitz *Solving the Shortest Vector Problem in 2^n Time via Discrete Gaussian Sampling*. In *STOC*, 2015.
- [2] M. Ajtai. *Generating hard instances of lattice problems*. Complexity of computations and proofs, volume 13 of *Quad. Mat.*, pages 1-32. Dept. Math., Seconda Univ. Napoli, Caserta, 2004.
- [3] M. Ajtai, R. Kumar, D. Sivakumar. *A sieve algorithm for the shortest lattice vector problem*. In *STOC*, pages 601-610, 2001.
- [4] J. Alwen, C. Peikert *Generating Shorter Bases for Hard Random Lattices* *Theory of Computing Systems*, April 2011, Volume 48, Issue 3, pp. 535-553
- [5] D. Aharonov, O. Regev. *Lattice problems in NP intersect coNP*. *Journal of the ACM*, 52(5):749-765, 2005.
- [6] Arora, Sanjeev et al. (1997). *The hardness of approximate optima in lattices, codes, and systems of linear equations*. *J. Comput. Syst. Sci.* 54 (2): 317-331.
- [7] L. Babai. *On Lovasz' lattice reduction and the nearest lattice point problem*. *Combinatorica*, 6(1):1-13, 1986.
- [8] W. Banaszczyk. *New bounds in some transference theorems in the geometry of numbers*. *Mathematische Annalen*, 296(4):625-635, 1993.
- [9] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, D. Stehle. *Classical hardness of learning with errors*. In *STOC*, pages 575-584, 2013.
- [10] J. Blomer, J.P. Seifert. *On the complexity of computing short linearly independent vectors and short bases in a lattice*. In *Proceedings of the 31st Annual ACM Symposium on Theory of Computing - STOC '99*, pages 711-720, Atlanta, GA, USA, May 1999. ACM.
- [11] A. Bogdanov, L. Trevisan. *On worst-case to average-case reductions for NP problems*. In *Proc. 44th Annual IEEE Symp. on Foundations of Computer Science (FOCS)*, pages 308-317, 2003.
- [12] J. Cai *On the average-case hardness of CVP* 42nd IEEE Symposium on Foundations of Computer Science, 2001. *Proceedings*. pp. 308 - 317, Oct. 2001
- [13] I. Dinur, G. Kindler, R. Raz, S. Safra *Approximating CVP to Within Almost-Polynomial Factors is NP-Hard*. *Combinatorica* 23 (2): 205-243., (2003).
- [14] O. Goldreich, S. Goldwasser. *On the limits of nonapproximability of lattice problems*. *Journal of Computer and System Sciences*, 60(3):540-563, 2000. Preliminary version in *STOC* 1998.
- [15] V. Guruswami, D. Micciancio, O. Regev. *The complexity of the covering radius problem*. *Computational Complexity*, 14:90-121, 2005. Preliminary version in *CCC* 2004.
- [16] O. Goldreich, D. Micciancio, S. Safra, J.P. Seifert *Approximating shortest lattice vectors is not harder than approximating closest lattice vectors*. *Inf. Process. Lett.* 71 (2): 55-61, 1999.

- [17] C. Gentry, C. Peikert, V. Vaikuntanathan *Trapdoors for hard lattices and new cryptographic constructions* *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pp 197-206., STOC 2008.
- [18] N. Howgrave-Graham *Approximate Integer Common Divisors* *Cryptography and Lattices* ,Volume 2146 of the series *Lecture Notes in Computer Science* pp 51-66, 2001.
- [19] I. Haviv, O. Regev. *Tensor-based hardness of the shortest vector problem to within almost polynomial factors.* *Theory of Computing*, 8(23):513-531, 2012.
- [20] S. Khot. *Hardness of approximating the shortest vector problem in lattices.* *Journal of the ACM*, 52(5):789-808, September 2005.
- [21] A. K. Lenstra, H. W. Lenstra, Jr. L. Lovasz. *Factoring polynomials with rational coefficients.* *Math. Ann.*, 261(4):515-534, 1982.
- [22] D. Micciancio. *The shortest vector problem is NP-hard to approximate to within some constant.* *SIAM Journal on Computing*, 30(6):2008-2035, March 2001.
- [23] D. Micciancio, C. Peikert *Hardness of SIS and LWE with Small Parameters.* *Crypto 2013* (Santa Barbara, CA, USA. August 2013.) Springer LNCS 8042, pp. 21-39.
- [24] D. Micciancio, O. Regev. *Worst-case to average-case reductions based on Gaussian measures.* *SIAM J. Comput.*, 37(1):267-302 (electronic), 2007.
- [25] J. E. Mazo , A. M. Odlyzko. *Lattice points in high-dimensional spheres.* *Monatshefte für Mathematik*, 110(1):47-61, March 1990.
- [26] O. Regev *On Lattices, Learning with Errors, Random Linear Codes, and Cryptography* *Journal of the ACM* 56(6), article 34, 2009.
- [27] O. Regev, N. Stephens-Davidowitz *Personal communication.*
- [28] C.P. Schnorr. *A hierarchy of polynomial time lattice basis reduction algorithms.* *Theoretical Computer Science*, 53(23):201- 224, 1987.
- [29] V. Vaikuntanathan *Personal communication.*